



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.                      | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|--------------------------------------|-------------|----------------------|---------------------|------------------|
| 10/023,622                           | 12/17/2001  | Jonathan Trostle     | 50325-0594          | 3947             |
| 29989                                | 7590        | 05/31/2006           | EXAMINER            |                  |
| HICKMAN PALERMO TRUONG & BECKER, LLP |             |                      | BERGER, AUBREY H    |                  |
| 2055 GATEWAY PLACE                   |             |                      |                     |                  |
| SUITE 550                            |             |                      | ART UNIT            |                  |
| SAN JOSE, CA 95110                   |             |                      | PAPER NUMBER        |                  |
|                                      |             |                      | 2134                |                  |

DATE MAILED: 05/31/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/023,622

Applicant(s)

TROSTLE ET AL.

Examiner

Aubrey H. Berger

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☐ Responsive to communication(s) filed on 16 March 2006.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-23 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-23 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### **DETAILED ACTION**

1. The response of 3/16/06 was received and considered.
2. Claims 1-23 are pending.

### ***Response to Arguments***

3. Applicant's arguments (pages 10-11) with respect to claims 1, 8, 15, and 22-23 have been considered but are moot in view of the new ground(s) of rejection.
4. In response to applicant's argument concerning claim 2 (page 12), the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).
5. In response to applicant's argument concerning claim 2 (page 12) that one of ordinary skill in the art would not be motivated to add additional, redundant, entries to a cache, a recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claim.
6. In response to applicant's arguments against the references individually, one cannot show nonobviousness by attacking references individually where the rejections

Art Unit: 2134

are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208

USPQ 871 (CCPA 1981); *In re Merck & Co.*, 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

***Claim Rejections - 35 USC § 103***

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1, 6-8, 13-15, and 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skene et al, hereinafter "Skene", (U.S. Patent Application Publication Number 2001/0052016) in view of Ye (U.S. Patent Number 6,772,348), in further view of Coss et al., hereinafter "Coss", (U.S. Patent Number 6,170,012).

Regarding claim 1, Skene discloses a computer system providing Internet protocol security without secure domain name resolution, the system comprising:

a local domain name service (DNS) server (Fig. 1, #110). Skene also discloses that a local DNS receives request messages including a domain name, after which the local DNS cache is searched to match the domain name (Fig. 4), but Skene lacks an IPSEC cache. However, Ye discloses a server (Col. 4, lines 8-14) communicatively computed to a processor/host-computer (Fig. 2, #70), that includes a secure Internet security

protocol (IPSEC) cache/cache table (Fig. 2, #120), wherein the secure IPSEC cache/cache table, is readable only by an Internet protocol (IP) processing layer/IPSEC driver (Fig. 2, #72), of an operating system that controls execution of an application program by the processor/host computer, (Col. 5, lines 50-54), a security policy data store/policy agent (Fig. 2, #90), that is communicatively coupled to the IP processing layer/IPSEC driver, a computer-readable medium accessible to the processor/host computer, and comprising one or more sequences of instructions which, when executed by the processor/host computer, cause the processor/host computer, to carry out the steps of: receiving a message/incoming packet (Fig. 4, #84), generated as a result of execution of the application program that contains a domain name (Fig. 6, #160), searching the secure IPSEC cache/cache table, for an entry that matches the domain name (Fig. 6, #164). Ye lacks wherein the searching comprises verifying that the domain name in the entry matches the domain name contained in the message. However, Coss discloses wherein the searching comprises verifying that the domain name in the entry matches the domain name contained in the message (Coss, fig. 5, #502-504). Ye discloses querying the security policy data store/policy agent, for an IPSEC policy/SA (Security Association) (Ye, Fig. 4, #136), matching the domain name (Ye, Fig. 6, #166). Ye lacks wherein the IP processing layers verifies that the policy matches the domain name contained in the message. However, Coss discloses wherein the IP processing layers verifies that the policy matches the domain name contained in the message (fig. 5, #502-504). Ye discloses applying the IPSEC policy/SA, to the message/incoming packet, (Ye, Fig. 6, #178), and purging the

Art Unit: 2134

matching entry from the cache (Ye, Fig. 6, #180), wherein the secure IPSEC cache/cache table, comprises a plurality of cache entries (Ye, Fig. 4, #124).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Skene's client (fig. 1, #112), to include a processor, security policy data store, IPSEC cache, and a computer-readable medium as described by Ye. One of ordinary skill in the art would have been motivated to perform such a modification to provide a method for retrieving security policies at an enhanced speed as taught by Ye (col. 2, lines 17-32).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Skene as modified above by Ye, with the device of Coss, in order to verify the domain name in the policy entry matches the domain name in the packet, in order to validate the packet may securely pass through the firewall as taught by Coss (col. 6, lines 16-25).

Regarding claim 6, Skene as modified above, discloses a computer system as recited in claim 1, further comprising the step of querying the security policy database/policy agent, for an IPSEC policy/SA, based on an IP address (Ye, Col. 2, lines 26-32 & Col. 7, lines 5-9). The invention of Ye discloses a system that derives an index value based on a packet's IP address (Ye, Col. 7, lines 5-9). The index value is used to search for a matching SA from the cache table (Ye, Col. 7, ¶5 to Col. 8, ¶1).

Art Unit: 2134

Regarding claim 7, Skene as modified above, discloses a computer system as recited in claim 1, further comprising the steps of: receiving a request to resolve a DNS name into network addresses/IP address, resolving the DNS name using the local DNS server (Fig. 4, #202), resulting in generating one or more network addresses/IP addresses, corresponding to the DNS name, determining identifier information/filter flag, that uniquely associates the request with a particular application process or execution time/communication stream, and storing the DNS name, the network addresses/IP addresses, and the identifier information/filter flag, as an entry in the secure IPSEC cache/cache table, (Col. 7, lines 9-36).

Claim 8 is substantially equivalent to claim 1 and therefore rejected under similar rational.

Claims 13-14 are substantially equivalent to claims 6-7 and therefore rejected under similar rational.

Regarding claims 15 and 22, Skene discloses a computer-readable medium carrying one or more sequences of instructions for providing Internet protocol security without secure domain name resolution, which instructions, when executed by one or more processors/host computer, cause the one or more processors/host computer, to carry out the steps of: receiving a message/incoming packet, generated as a result of execution of an application program/communication stream, and that contains a domain

Art Unit: 2134

name (Fig. 4, #202), searching a secure Internet security protocol (IPSEC) cache/cache table, for an entry that matches the domain name (Fig. 4, #203). Skene lacks wherein the searching comprises verifying that the domain name in the entry matches the domain name contained in the message. However, Coss discloses wherein the searching comprises verifying that the domain name in the entry matches the domain name contained in the message (Coss, fig. 5, #502-504). Skene discloses wherein the secure IPSEC cache/cache table, is communicatively coupled to a local domain name service (DNS) server (Fig. 1, #110), and wherein the secure IPSEC cache/cache table, is readable only by an Internet protocol (IP) processing layer/IPSEC driver, of an operating system that controls execution of the application program/communication stream, querying a security policy data store/policy agent, that is communicatively coupled to the IP processing layer/IPSEC driver, for an IPSEC policy/SA, matching the domain name (Ye, Fig. 6, #166). Ye lacks wherein the IP processing layers verifies that the policy matches the domain name contained in the message. However, Coss discloses wherein the IP processing layers verifies that the policy matches the domain name contained in the message (fig. 5, #502-504). Ye discloses applying the IPSEC policy/SA, to the message/incoming packet, and purging the matching entry from the cache (Ye, Fig. 6, #180).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Skene's client (fig. 1, #112), to include a processor, security policy data store, IPSEC cache, and a computer-readable medium as described by Ye. One of ordinary skill in the art would have been motivated to perform such a modification to



provide a method for retrieving security policies at an enhanced speed as taught by Ye (col. 2, lines 17-32).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Skene as modified above by Ye, with the device of Coss, in order to verify the domain name in the policy entry matches the domain name in the packet, in order to validate the packet may securely pass through the firewall as taught by Coss (col. 6, lines 16-25).

Claims 20-21 are substantially equivalent to claims 6-7 and therefore rejected under similar rationale.

Regarding claim 23, Skene discloses an apparatus for providing Internet protocol security, without secure domain name resolution, for messages that are carried by a packet-switched data network (Ye, Fig. 2), comprising: a network interface that is coupled to the data network for receiving one or more packet flows therefrom (Ye, Fig. 2, #84), a processor/host computer, one or more stored sequences of instructions which (Ye, Col. 3, lines 2-4), when executed by the processor/host computer, cause the processor/host computer, to carry out the steps of: receiving a message/incoming packet, generated as a result of execution of an application program/communication stream, and that contains a domain name (Page 4, Col. 1, lines 17-20), searching a secure Internet security protocol (IPSEC) cache/cache table, for an entry that matches

Art Unit: 2134

the domain name (Ye, Fig. 6, #164). Ye lacks wherein the searching comprises verifying that the domain name in the entry matches the domain name contained in the message. However, Coss discloses wherein the searching comprises verifying that the domain name in the entry matches the domain name contained in the message (Coss, fig. 5, #502-504). Ye discloses wherein the secure IPSEC cache/cache table, is communicatively coupled to a local domain name service (DNS) server (Fig. 1, #110), and wherein the secure IPSEC cache/cache table, is readable only by an Internet protocol (IP) processing layer/IPSEC driver, of an operating system that controls execution of the application program, (Ye, Col. 5, lines 50-54), querying a security policy data store/policy agent, that is communicatively coupled to the IP processing layer/IPSEC driver, for an IPSEC policy, matching the domain name (Ye, Fig. 6, #166). Ye lacks wherein the IP processing layers verifies that the policy matches the domain name contained in the message. However, Coss discloses wherein the IP processing layers verifies that the policy matches the domain name contained in the message (fig. 5, #502-504). Ye discloses applying the IPSEC policy/SA to the message/incoming packet (Ye, Fig. 6, #178), and purging the matching entry from the cache (Ye, Fig. 6, #180).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Skene's client (fig. 1, #112), to include a processor, security policy data store, IPSEC cache, and a computer-readable medium as described by Ye. One of ordinary skill in the art would have been motivated to perform such a modification to

Art Unit: 2134

provide a method for retrieving security policies at an enhanced speed as taught by Ye (col. 2, lines 17-32).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Skene as modified above by Ye, with the device of Coss, in order to verify the domain name in the policy entry matches the domain name in the packet, in order to validate the packet may securely pass through the firewall as taught by Coss (col. 6, lines 16-25).

4. Claims 2-5, 9-12, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Skene in view of Ye and further in view of Coss, as applied to claim 1 above, and further in view of Dixon et al, hereinafter "Dixon", (U.S. Patent Number 6,697,857).

Regarding claim 2, Skene as modified above discloses a computer system as recited in claim 1. However, Skene as modified above, lacks wherein each cache entry comprises a DNS name. Dixon discloses wherein each cache entry comprises a DNS name (Col. 7, line 1), one or more corresponding IP addresses, and information that uniquely associates the cache entry with a particular application process or execution time (Skene, Col. 6, lines 51-60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the device of Skene as modified

Art Unit: 2134

above, with the device of Dixon in order to include a DNS name in the cache entry because DNS names are text names corresponding to the numeric IP address.

Regarding claims 3 and 4, Skene as modified above, discloses a computer system as recited in claim 2, wherein the step of searching the secure IPSEC cache/cache table, further comprises the step of searching the secure IPSEC cache/cache table, for an entry that matches a process identifier/filter flag (Ye, Fig. 4, #136), of the application program (Ye, Col. 6, lines 56-60), based on the information that uniquely associates the cache entry with a particular application process or execution time/communication stream (Ye, Col. 7, ¶3), wherein the information that uniquely associates the cache entry with a particular application process or execution time/communication stream, comprises a process identifier value/filter flag, and a transaction identifier value/index value (Ye, Fig. 6, #162).

Regarding claim 5, Skene as modified above, discloses a computer system as recited in claim 4, wherein the step of searching the secure IPSEC cache/cache table, further comprises the step of searching the secure IPSEC cache/cache table, for an entry that matches a process (Ye, Fig. 6, #168) and transaction (Ye, Fig. 6, #162) associated with the application program/communication stream, based on the process identifier value/filter flag, and transaction identifier value/index value, in the cache.

Art Unit: 2134

Claims 9-12 are substantially equivalent to claims 2-5 and therefore rejected under similar rationale.

Claims 16-19 are substantially equivalent to claims 2-5 are therefore rejected under similar rationale.

### ***Conclusion***

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aubrey H. Berger whose telephone number is (571)272-

Art Unit: 2134

8155. The examiner can normally be reached on Monday - Thursday, 9:00 a.m. - 6:30 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jacques Louis-Jacques can be reached on (571)272-6962. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

AHB

AHB

*Jacques Louis-Jacques*  
JACQUES H. LOUIS-JACQUES  
PRIMARY EXAMINER